Office of the Information and Privacy Commissioner for Nova Scotia

---

INVESTIGATION REPORT IR16-01

Office of the Premier

Catherine Tully
Information and Privacy Commissioner for Nova Scotia
February 11, 2016

TABLE OF CONTENTS

	Page
Commissioner's Message	3
Executive Summary	5
1.0 Purpose & Scope	7
1.1 Background	7
1.2 Jurisdiction	7
1.3 Investigative process	8
2.0 Issues	8
3.0 Analysis and Findings	9
3.1 Does *FOIPOP* apply to the Premier's chief of staff?	9
3.2 If *FOIPOP* applies, was the disclosure authorized?	11
3.3 Were reasonable steps taken in response to the privacy breach?	15
1. Breach containment	15
2. Risk evaluation – cause and extent of the breach	15
3. Notification	20
4. Prevention	20
4.0 Summary of Findings and Recommendations	25
5.0 Conclusion	26
6.0 Acknowledgments	26
Appendix 1	29

Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner (Review Officer)
Catherine Tully

INVESTIGATION REPORT

February 11, 2016

Office of the Premier

Commissioner's Message

This investigation arises out of what might best be described as a series of unfortunate events that culminated in the dismissal of a cabinet minister and the resignation of the Chief of Staff to the Premier. This investigation focussed on the disclosure of personal health information to the media by the Chief of Staff on November 23, 2015.

Whenever government officials find their decisions challenged and subject to public scrutiny there is pressure to be transparent and accountable to the public. If part of the explanation includes the personal information of a third party, that information can only be disclosed if authorized under the *Freedom of Information and Protection of Privacy Act* ("*FOIPOP*").

Personal health information, particularly mental health information is among the most sensitive personal information. Although much progress has been made in recent years there remains a stigma associated with mental illness so much so that individuals often do not disclose their illness even to close family members. As a society our laws reflect our understanding of the sensitivity of this type of information. There are strict rules governing its disclosure by public bodies. It will be a rare circumstance when disclosure of sensitive medical information to the media is authorized under our privacy laws.

Privacy protections safeguard democratic societies by furthering autonomy, self-fulfillment, and freedom.[1] Public bodies must be constantly vigilant to ensure that their privacy controls are current and effective.

[1] For an interesting discussion on this and other ideas about the meaning of privacy in modern society see, Jathan Sadowski, "*Why Does Privacy Matter: One Scholar's Answer*", *The Atlantic* (26 February 2013): http://www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/.

Our investigation revealed shortcomings in the design and implementation of privacy practices and procedures in the Office of the Premier and across government generally. It revealed that there is work to be done within government to ensure that all employees are aware of the fundamental importance of privacy in our society and the privacy rules that govern their activities as employees of public bodies. As a result, I have set out six specific recommendations that, when implemented, will ensure the government has established the foundation for a strong, modern privacy management program. During the investigation government officials confirmed that significant work is already underway to update and improve the government's privacy management program.

My office has issued many guidance documents on how to build an effective and modern privacy management program. For example last year we posted a summary of the essential elements of a privacy management program and a step-by-step gap analysis guide so that public bodies can measure their progress in building an effective program.[2]

My expectation is that this report will prompt not only government departments but other public bodies generally to re-evaluate the quality and effectiveness of their privacy management programs with a view to ensuring that they have in place controls and leadership ready to face the challenges of managing the ever growing collections of personal information entrusted to them.

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

[2] Privacy management tools on our website include a summary of the essential elements of a privacy management program, a gap analysis tool for smaller public bodies, a gap analysis tool for health custodians in three phases and a gap analysis tool for larger public bodies: http://foipop.ns.ca/publicbodytools.

Executive Summary

[1] In November, 2015, a secretly recorded conversation between Kirby McVicar, then the Premier's Chief of Staff, and former Cabinet Minister Andrew Younger surfaced. The tape gave rise to allegations that Mr. McVicar was offering Katia Younger, Mr. Younger's wife, a personal services contract. This generated intense media interest and speculation which, in turn, placed a great deal of pressure on the government to respond.

[2] In a series of media interviews conducted on November 23, 2015, Mr. McVicar explained his words on the tape. His explanation was that Mr. Younger was under significant pressure at the time of the conversation. To provide evidence of this pressure, Mr. McVicar disclosed sensitive personal information, including health information, of Mr. Younger. This report finds that the disclosure was a breach of the privacy rules in the *FOIPOP Act*.

[3] Our investigation revealed that there were three contributing factors to the disclosure of the personal information: public pressure to explain references to personal services contracts, a lack of privacy training and awareness, and a lack of media preparation and experience. The report highlights three main concerns from a privacy perspective. First, the evidence revealed that neither Mr. McVicar nor the Communications Director for the Office of the Premier had received any privacy training; second, they were not familiar with the office's privacy policies; third, they were unaware of who the privacy lead or resource in the Office of the Premier was. These factors significantly contributed to the unauthorized disclosure of personal information.

[4] This investigation presents an opportunity to government. A modern privacy management program is essential to effectively managing the collection, use and disclosure of personal information. This is especially important given the recent exponential growth in our abilities to collect, use, disclose and store personal information. Our investigation finds that the privacy management program at the Office of the Premier and across government falls short of a full, effective, modern program. We make six recommendations that will move the province closer to this ideal:

Recommendation #1: Breach Notification

[5] That within 30 days of receipt of this report the Office of the Premier:

- provide this office with its response to the recommendations in this report, including timelines for implementation of each recommendation;
- publish its response to the recommendations in this report on its website.

Recommendation #2: Personal Services Contracts

[6] That the standard personal services contract template be updated to add provisions (privacy protection schedule) that:

- clearly state that information obtained by virtue of service to the government is subject to Nova Scotia's access and privacy laws,
- require contractors to complete privacy training within one month of signing of contract and,

- require contractors to sign confidentiality agreements that clearly reference *FOIPOP* access and privacy rules.

Recommendation #3: Non-Disclosure Agreements

[7] That the Employee Non-Disclosure Agreement template be amended to make specific reference to the requirement to protect personal information.

Recommendation #4: Privacy Policy

[8] That the Office of the Premier's privacy policy including the breach management protocol be updated to:

- more clearly identify the circumstances in which personal information is collected, used and disclosed by that Office,
- modernize any references to reasonable security standards, and
- update the privacy breach protocol to reflect modern breach management standards.

Recommendation #5: Privacy Training

[9] That basic privacy training:

- be made mandatory for all government employees and that attendance be monitored;
- be updated to include core elements of: identifying personal information, understanding the basic rules of when employees are authorized to collect, use or disclose personal information, recognizing a potential privacy issue or breach and knowing exactly to whom employees can address their privacy questions to avoid problems. The training should also include essential modern security requirements including end of day procedures, secure destruction of personal information, travelling with personal information and transmitting personal information;
- be periodically refreshed as a mandatory requirement that is monitored and enforced.

Recommendation #6: Chief Privacy Officer

[10] That the Office of the Premier and other government public bodies appoint an executive level Chief Privacy Officer to provide strategic privacy leadership.

[11] In one month we will follow up with the Office of the Premier for an update on how it is implementing the recommendations in this report.

1.0 Purpose & Scope

1.1 Background

[12] On November 23, 2015, Kirby McVicar, then the Chief of Staff to the Premier, granted a series of media interviews in relation to a taped conversation between himself and Andrew Younger, a former Liberal MLA and Cabinet Minister.

[13] Reports of the interview began appearing on television and in print through November 23 and November 24. Media reports consistently reported that Mr. McVicar disclosed the following information:

- "Mr. Younger indicated to me he had a brain tumour."
- "Mr. Younger indicated to me that he had PTSD."
- "His wife was about to be laid off from the school she was working at."[3]

[14] On November 24, 2015, Mr. McVicar resigned his position as Chief of Staff over concerns that his disclosure of information on November 23, 2015 had violated Nova Scotia's privacy laws.

[15] In a letter received by this office on November 25, 2015, Mr. Younger filed a complaint regarding the disclosure of his personal health information by Mr. McVicar.

1.2 Jurisdiction

[16] As the Information and Privacy Commissioner for Nova Scotia I have the statutory mandate to monitor public bodies' compliance with the privacy rules in the *Freedom of Information and Protection of Privacy Act ("FOIPOP")* to ensure that the law's purposes are achieved.[4] Under the *Privacy Review Officer Act* ("*PRO Act*") I can receive and investigate complaints or I can initiate privacy investigations if "there are reasonable grounds to believe that a person has contravened or is about to contravene the privacy provisions and the subject-matter of the review relates to the contravention."[5]

[17] The purposes of *FOIPOP* are to ensure that public bodies are fully accountable to the public, in part, by preventing the unauthorized collection, use or disclosure of personal information by public bodies. *FOIPOP* is intended to protect the privacy of individuals with respect to the personal information about themselves held by public bodies.[6]

---

[3] See for example Sarah Ritchie, *CTV News Atlantic* (23 November 2015) http://atlantic.ctvnews.ca/video?clipId=757032 ; Jean LaRoche, *CBC News Nova Scotia* (23 November 2015) http://www.cbc.ca/player/play/2679402300; Michael Gorman, *Chronicle Herald* (23 November 2015) http://thechronicleherald.ca/novascotia/1323809-mcvicar-job-offer-to-younger%E2%80%99s-wife-meant-to-relieve-stress; Marieke Walsh, *Global News* (24 November 2015) http://globalnews.ca/news/2358517/andrew-younger-files-complaint-with-privacy-commissioner-after-personal-health-information-revealed/.

[4] I have been appointed as the Review Officer under s. 33(1) of the *Freedom of Information and Protection of Privacy Act* and the Privacy Review Officer under s. 4(1) of the *Privacy Review Officer Act*.

[5] *Privacy Review Officer Act*, s 5(1)(b).

[6] *FOIPOP* ss. 2(a)(iv), 2(c).

[18] In this case, when I received Mr. Younger's privacy complaint, there was already extensive media coverage regarding what appeared to be an unauthorized disclosure of personal information. As a result, I decided to initiate an investigation of privacy compliance because, in my view, there were reasonable grounds to believe that a person may have contravened the privacy provisions of *FOIPOP*.[7] My office notified the Office of the Premier of our intention to conduct an investigation on November 25, 2015.

1.3 Investigative process

[19] My investigators conducted a series of interviews with 10 individuals including Andrew Younger, Katia Younger and Kirby McVicar - the former Chief of Staff, Office of the Premier. We interviewed three other staff with responsibilities in the Office of the Premier: the Communications Director in the Office of the Premier, the Executive Director of the Executive Council Office and the Director of Operations and Administration for the Office of the Premier. To better understand privacy training in the area of communications we interviewed the Associate Deputy Minister of Communications Nova Scotia. Finally, we interviewed three individuals who work in the new centralized access and privacy operations for government in the Department of Internal Services: the Chief Information Access and Privacy Officer, the Systems Privacy Specialist, and the Corporate Information Access & Privacy Administrator with responsibilities for the Office of the Premier.

[20] As part of this investigation we reviewed the privacy policies, practices and procedures used by the Office of the Premier and the government generally. We obtained and reviewed copies of all of the privacy training materials used to train Office of the Premier staff, deputy ministers and ministers since October, 2013. We also gathered documentary evidence in relation to the information provided by the witnesses. Finally, we conducted a review of all available media reports in relation to the disclosure of information about Mr. and Mrs. Younger.

2.0 Issues

[21] The issues arising from this investigation are:

(1) Does *FOIPOP* apply to the Premier's chief of staff?
(2) If *FOIPOP* applies, was the disclosure authorized?
(3) Were reasonable steps taken in response to the privacy breach?

[7] Privacy investigations can be initiated by the Review Officer pursuant to s. 5(1)(b) of the *Privacy Review Officer Act*. Section 5(2) of the *Privacy Review Officer Act* states that the Review Officer may only exercise her powers to investigate a complaint after the person who has made the complaint has completed the use of the internal privacy-complaint procedure of the public body to which the complaint was made. Because I chose to initiate the investigation, the complainant was not required to take this step.

3.0 Analysis and Findings

3.1 Does *FOIPOP* apply to the Premier's chief of staff?

[22] The Office of the Premier is a public body for the purposes of *FOIPOP*[8] and as such, records in the custody or control of the Office of the Premier, including personal information are all subject to the access and privacy rules in that *Act*.

[23] The mandate of the Office of the Premier is described in the Corporate Administrative Policy Manual, Management Guide:[9]

> **Office of the Premier**
> The Office of the Premier supports the Premier in carrying out the functions demanded of the head of government, leader of a political party, and Member of the House of Assembly. Its staff are primarily appointed by the Premier.
>
> Premier's Office staff provide the Premier with policy and political advice; they also deal with day-to-day matters in the legislature and ensure political liaison with Caucus and the party.
>
> The office also provides practical administrative support for the Premier, including coordinating his agenda, travel and media relations and preparing correspondence.

[24] The policy makes clear that the Office of the Premier, as a public body, engages in a wide range of activity including policy and political advice, media relations and political liaison.

[25] *FOIPOP* provides that an "employee", in relation to a public body, includes a person retained under an employment contract to perform services for the public body.[10] In addition, in accordance with the Office of the Premier's privacy policy, all employees must abide by the legislated obligations under *FOIPOP*. The policy states that employees include individuals under a personal services contract.[11] The Chief of Staff to the Premier signed a personal services contract with the province on October 22, 2013.

---

[8] "Public body" is defined in s. 3(1)(j) of *FOIPOP* and includes government departments. "Departments" are not defined in *FOIPOP* but they are defined in the *General Civil Service Regulations* under the *Civil Service Act*. Schedule A to that regulation lists all departments and included in that list is the Office of the Premier.

[9] Corporate Administrative Policy Manual, Management Guide Chapter 2 p. 12: http://novascotia.ca/treasuryboard/manuals/100MgmtGuide.htm.

[10] *FOIPOP* s. 3(1)(e).

[11] Privacy Policy - Office of the Premier, Effective Date April 1, 2009 – "Definitions – For the purposes of this policy, the following definitions shall apply. Employee – an individual in the employ of, seconded to, or under personal service contract to the Office of the Premier and its volunteers, students and interns who have access to records." As of February 3, 2016, the web link to the Office of the Premier's Privacy Policy was misdirecting to Communications NS; staff informed us that the link would soon be restored. http://premier.novascotia.ca/

[26] Therefore, I find that Mr. McVicar, in his role as Chief of Staff to the Premier, was an employee of the Office of the Premier for the purposes of *FOIPOP* and that as such, his collection, use and disclosure of personal information in that role was subject to the *FOIPOP* rules.[12]

[27] The duties of the chief of staff are not enumerated in the services contract. Mr. McVicar explained that his primary role was to make sure the Premier is fully staffed, fully briefed, and to liaise between the Premier and the caucus, the Premier and the cabinet and the Premier and the deputy ministers. He sat in on most meetings with the Premier and monitored any follow-up actions from those meetings. With respect to the cabinet in particular, the chief of staff must ensure that cabinet ministers are in essence ready, willing and able to perform that function. As part of that role the chief of staff receives and reviews medical information regarding the medical fitness of potential and serving cabinet ministers. As Chief of Staff, one of his other duties also included approval of leave, travel and vacation of ministers.

[28] Mr. Younger's evidence confirmed that he had provided detailed health information to the Office of the Premier. He understood the purpose for the collection of the personal health information of ministers was to make the Premier's Office aware of any health issues that could impact the ability of a minister to serve – including such things as the ability to travel, to ensure attendance at meetings and in the House for quorum, as well as to know if there would be a need to appoint someone to act in the place of a minister.

[29] The evidence establishes that the collection, use and disclosure of the personal health information of current and potential cabinet ministers by the Chief of Staff was part of his employment obligations under his personal services contract. As such, I find that these activities were subject to the access and privacy rules under *FOIPOP*.[13]

[30] This finding is consistent with the important public interest purposes of *FOIPOP* as well. It is in the public interest that potential candidates for cabinet positions are thoroughly vetted to ensure their suitability for the position. It is also in the public interest that candidates can confidently disclose all relevant and necessary information – warts and all so to speak. This will ensure that the best possible candidates are selected and that any risks to the public interest in the selection can be adequately addressed. If the information supplied by these potential cabinet ministers were not subject to the privacy and security protections of *FOIPOP*, this could significantly undermine the willingness of these candidates to be as forthright and honest as

---

[12] I note that this finding is also consistent with the fact that it is not possible to contract out of *FOIPOP*. Any records in the custody and control of a public body are subject to the rules in *FOIPOP*. For a recent discussion of this point see *Imperial Oil v. Alberta IPC* 2014 ABCA 231 at para. 75 where the court states, "The Commissioner made the obvious point that no public body can "contract out" of the FOIPOP Act. No party disputes that…".

[13] The activities of chiefs of staffs to ministers and premiers have come under increasing scrutiny by Commissioners in recent years. Last year the Saskatchewan Privacy Commissioner determined that the Chief of Operations and Communication for the Office of the Premier was not subject to FOIPOP because of a unique exclusion in the Saskatchewan law for members of the Executive Council. Last month in British Columbia the Privacy Commissioner determined that the activities of the Chief of Staff to a minister and the Deputy Chief of Staff to the Premier were subject to the FOIPOP rules in that jurisdiction. See Investigation Report 092-2015 (Saskatchewan) at para. 82-83 and Investigation Report F15-03 (British Columbia). Nova Scotia's FOIPOP, like British Columbia's law, does not have an exclusion for members of Executive Council.

possible during the vetting process. There is therefore, not only a legal reason for why *FOIPOP* applies to this information, there is a public interest reason as well.

[31] There was some discussion as to whether or not the *Personal Health Information Act* ("*PHIA*") applied because some of the information at issue qualified as personal health information within the meaning of that *Act*. *PHIA* only applies to the collection of personal information by a custodian and the disclosure of personal information by a custodian or a person to whom a custodian disclosed the information. "Custodian" is defined in *PHIA* and consists of a limited group including mainly regulated health professionals. Since the disclosure in this case did not involve a custodian, *PHIA* does not apply.

3.2 If *FOIPOP* applies, was the disclosure authorized?

[32] To determine whether or not the disclosure was authorized I must answer two questions:

a. Was the information "personal information" within the meaning of *FOIPOP*?
b. If so, was the disclosure authorized under *FOIPOP*?

[33] The facts in this case are not in dispute. On Monday November 23, 2015, Mr. McVicar, then the Chief of Staff for the Premier, gave a number of media interviews. At least seven media outlets reported what Mr. McVicar said in those interviews and the reports are quite consistent in terms of the nature of the information he disclosed. For the purposes of this investigation it is the following three pieces of information that are at issue:

- "Mr. Younger indicated to me he had a brain tumour."
- "Mr. Younger indicated to me that he had PTSD."
- "His wife was about to be laid off from the school she was working at."[14]

a. Was the disclosed information "personal information"?

[34] For the privacy rules in *FOIPOP* to apply, the information must qualify as "personal information" within the meaning of the *Act*:

> 3(1) In this Act,
> (i) "personal information" means recorded information about an identifiable individual, including
> (i) the individual's name, address or telephone number,
> (ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,

[14] See for example Sarah Ritchie, *CTV News Atlantic* (23 November 2015) http://atlantic.ctvnews.ca/video?clipId=757032; Jean LaRoche, *CBC News Nova Scotia* (November 23 2015) http://www.cbc.ca/player/play/2679402300; Michael Gorman, *Chronicle Herald* (November 23 2015) http://thechronicleherald.ca/novascotia/1323809-mcvicar-job-offer-to-younger%E2%80%99s-wife-meant-to-relieve-stress; Marieke Walsh, *Global News* (November 24 2015) http://globalnews.ca/news/2358517/andrew-younger-files-complaint-with-privacy-commissioner-after-personal-health-information-revealed/.

(iii) the individual's age, sex, sexual orientation, marital status or family status,
(iv) an identifying number, symbol or other particular assigned to the individual,
(v) the individual's fingerprints, blood type or inheritable characteristics,
(vi) information about the individual's health-care history, including a physical or mental disability,
(vii) information about the individual's educational, financial, criminal or employment history,
(viii) anyone else's opinions about the individual, and
(ix) the individual's personal views or opinions, except if they are about someone else;

[35] Subparagraph (vi) of this definition states that personal information includes information "about" health-care history including a physical or mental disability. The information disclosed by Mr. McVicar was two medical diagnoses. As such I find that the information disclosed was personal information within the meaning of *FOIPOP*.

[36] Mr. Younger's evidence was that one of the disclosed medical diagnoses was not true. Does this make the information not the personal information of an individual? Subparagraph (vi) of the definition above says only that the information must be "about" the individual's health-care history. According to the Concise Oxford English Dictionary, "about" means "on the subject of; concerning".[15] From a logical perspective it would not make sense that *FOIPOP* only applied to disclosures of true or accurate personal information since inaccurate information can be as harmful to personal privacy as accurate information. *FOIPOP* includes a right to request a correction of personal information which clearly suggests that inaccurate information can qualify as personal information.[16] Other jurisdictions have accepted that inaccurate information about an applicant falls within the definition of "personal information".[17] Finally, I note that in *R. v. Morris*, the Nova Scotia Provincial Magistrate's Court found the accused guilty of disclosing personal information contrary to s. 6(2) of the predecessor to our current *FOIPOP* even though the disclosed information was not accurate.[18]

[37] I conclude that the accuracy of the information does not affect whether or not the information qualifies as "personal information" within the meaning of *FOIPOP* so long as the disclosure was intended to be "about" the individual.

[38] With respect to Mrs. Younger, Mr. McVicar disclosed that she "was about to be laid off from the school she was working at." Does this qualify as a personal information? Mr. and Mrs. Younger gave evidence that the information was communicated by Mr. Younger as a concern both he and Mrs. Younger had in December, 2014. The information was in fact only the opinion of Mr. and Mrs. Younger. Mrs. Younger was not laid off. As noted above, the definition of

---

[15] *Concise Oxford English Dictionary*, 12th ed., p. 4.
[16] *FOIPOP* s. 25.
[17] Ontario IPC Order PO-1881-I at p. 6.
[18] *R. v. Morris* [1988] N.S.J. No. 383. The Court notes that Mr. Morris stated to the media that the complainant in that case was in receipt of municipal assistance but that she was not, at any time material to the matter, in receipt of social assistance under the family benefits section of the *Act*. Mr. Morris made the comments in response to what the court describes as a public castigation of the Minister by the complainant.

personal information includes an individual's personal views or opinions, except if they are about someone else (then they are that person's personal information). Therefore I find that the information that Mrs. Younger "was about to be laid off" was the opinion of a third party (both of Mr. and Mrs. Younger) and as such was their personal information.

b. Was the disclosure authorized under *FOIPOP*?

[39] The basic rule in *FOIPOP* is that public bodies may only disclose personal information in accordance with *FOIPOP*. Sections 27 and 31 of *FOIPOP* list the circumstances in which disclosure of personal information is authorized.[19]

[40] When a public body is responding to an access to information request the *FOIPOP* rules state that a public body must refuse to disclose third party personal information if the disclosure would be an "unreasonable invasion of third party's personal privacy". There are numerous cases on the meaning of this phrase and the *Act* itself provides detailed guidance on how to determine when a disclosure is an unreasonable invasion of personal privacy.[20]

[41] Where a disclosure of personal information occurs outside of the formal access to information process, as in this case, different rules apply. Based on these rules, where a public disclosure is made to the media the most likely authorities are: that the individual consented in writing to the disclosure; that compelling circumstances exist that affect anyone's health or safety, or; that the disclosure is clearly in the public interest.[21]

[42] The evidence from both Mr. McVicar and Mr. Younger was that Mr. Younger did not consent to the disclosure of his personal information. Mr. and Mrs. Younger confirmed that they did not consent to the disclosure of their opinion regarding Mrs. Younger's employment prospects.

[43] The second possible authority for a public disclosure of personal information would be if there were compelling circumstances that affected anyone's health or safety. There was no evidence from any witness that there were any health or safety issues relating to the disclosure.

[44] The final possible authority is that the disclosure was clearly in the public interest as set out in s. 31(1)(b) of *FOIPOP* which states:

> 31(1) Whether or not a request for access is made, the head of a public body may disclose to the public, to an affected group of people or to an applicant information
> (b) the disclosure of which is, for any other reason, clearly in the public interest.

---

[19] See Appendix 1 to this report for a summary of the circumstances where disclosure of personal information is permitted under *FOIPOP*.
[20] See *FOIPOP* s. 20. For a recent discussion of how to apply the four-part test in s. 20, see NS Review Reports FI-10-95 and FI-11-71.
[21] *FOIPOP* ss. 27(b), 27(o), 31(1)(b).

[45] The Supreme Court of Canada recently commented on the meaning of "public interest":

> To be of public interest, the subject matter "must be shown to be one inviting public attention, or about which the public has some substantial concern because it affects the welfare of citizens, or one to which considerable public notoriety or controversy has attached.[22]

[46] Recently, the Information and Privacy Commissioner for Saskatchewan enumerated a number of criteria for determining when a matter is of public interest.[23] In summary those criteria are:

1. Did the release of personal information contribute to the public understanding of or a debate or resolution of, a matter or issue that is of concern to the public or a sector of the public?
2. Did the release of personal information contribute to open, transparent and accountable government?
3. Did the individual whose personal information was released contribute in any way to placing this issue in the public eye?

[47] Saskatchewan's provision is slightly different from Nova Scotia's. However, I would include the fourth Saskatchewan criteria for Nova Scotia's purposes, consistent with best privacy practices and to ensure that any personal information released is "clearly" in the public interest:

4. Did the public interest in the disclosure outweigh the invasion of personal privacy? Included in this question is whether or not the minimum amount of personal information was disclosed to satisfy the public interest purpose.

[48] Applying those four criteria to this case I am satisfied that there was a public interest at stake. At the time of the disclosure by Mr. McVicar there was extensive media coverage and the debate in the House had become focused on the content of the tape recorded conversation. Opposition parties were demanding an explanation for what appeared to be an offer of a personal services contract. In this case, Mr. Younger himself contributed to placing the issue in the public eye by releasing the initial portion of the tape in the House. However, the actual personal information disclosed was highly sensitive personal health information. In my view, providing specific medical diagnoses was more than the minimum amount necessary. As a result I find that the disclosure of the personal information was not authorized under *FOIPOP*.

[49] No evidence or argument was offered suggesting that any other authority under *FOIPOP* permitted the disclosure. I have carefully reviewed all of the potential authorities for disclosure of the personal information and found no evidence that any other possible authority existed.

[50] As a result, I find that the disclosure of third party personal information by Mr. McVicar on November 23, 2015 was not authorized.

---

[22] Grant v. Torstar Corp., [2009] 3 SCR 640 at para. 105.
[23] Investigation Report 092-2015 to 095-2015 at para. 66.

3.3 Were reasonable steps taken in response to the privacy breach?

[51] A privacy breach occurs whenever there is an unauthorized collection, use, disclosure or destruction of personal information in the custody or control of a public body. Such activity is "unauthorized" if it occurs contrary to the provisions of *FOIPOP*. When a privacy breach occurs, public bodies must take immediate steps to manage the breach.

[52] The four key steps in managing a privacy breach are: [24]

1. Breach containment
2. Risk evaluation – cause and extent of the breach
3. Notification
4. Prevention

1. Breach containment

[53] The first, and often most important step in managing a privacy breach, is to immediately determine if anything can be done to stop the unauthorized practice. Shutting down a system that was breached, revoking or changing computer access codes or sending remote "kill" signals to lost or stolen portable storage devices are typical strategies.

[54] In this case the breach consisted of a series of statements to a number of media outlets. The disclosure of personal information was not recognized as an issue until after the information was widely published. The public body's containment strategy consisted of accepting Mr. McVicar's resignation. No further containment was possible given the circumstances of the breach.

2. Risk evaluation – cause and extent of the breach

[55] In order to evaluate what steps are necessary to manage the breach and to prevent future breaches, public bodies must evaluate the nature of the personal information involved, the cause and extent of the breach, and the foreseeable harm from the breach.

[56] In the initial announcements relating to Mr. Younger's leave, the Office of the Premier made clear that the leave was being taken so that Mr. Younger could deal with personal matters. Further, the press release at the time stated, "The premier's office will provide no details of the personal matters. That is for Mr. Younger to discuss, should he choose to do so."[25]

---

[24] My office has published a guide to managing privacy breaches entitled, "Key Steps to Responding to Privacy Breaches" available at http://foipop.ns.ca/sites/default/files/publications/Key%20Steps%20-%20Full%20-%20Final%20-%202015Oct27.pdf . This approach to breach management is consistent with numerous other jurisdictions in Canada and is based in particular on work done by the Office of the Information and Privacy Commissioner for British Columbia.

[25] Statement from the Premier's Office (26 January 2015): http://novascotia.ca/news/release/?id=20150106002.

[57] The Office of the Premier demonstrated a reasonable approach to explaining the need for Mr. Younger's leave early on. What, then, led the Chief of Staff to later disclose more of Mr. Younger's personal information? Based on the evidence provided by the witnesses, I find that a number of factors contributed to the unauthorized disclosure of personal information in this case:

- **Public pressure:** The Chief of Staff felt pressured to explain in particular why he had discussed a personal services contract with Mr. Younger. Part of the explanation related to the personal information of Mr. and Mrs. Younger.
- **Lack of privacy training and awareness:** Neither the Chief of Staff nor the Communications Director for the Office of the Premier had received any privacy training during their tenure in that office. Neither had read the privacy policy, knew who the privacy resources in the office were, nor knew with certainty whether they had signed a confidentiality agreement. As a result, both failed to recognize the potential for a privacy breach.
- **Lack of media preparation and experience:** When Mr. McVicar gave the media interviews on Nov. 23, 2015, he did so with only 10 minutes of media preparation from someone who reported directly to him. This was insufficient preparation given that he had not given a media interview in at least five years and that some of the background material involved sensitive personal information.

Cause of the breach – public pressure

[58] From late 2014 until November 2015, Mr. Younger's leave, resignation, return and subsequent dismissal from cabinet was a story of great interest in the media. After his final dismissal in November 2015, Mr. Younger produced portions of a tape recorded conversation between himself and Mr. McVicar from February 12, 2015. The tapes gave rise to further questions, particularly surrounding whether Mr. McVicar had offered a personal services contract to Mrs. Younger. Opposition parties and the media were pressuring the government to explain the conversation on the tape. Other than Mr. Younger, Mr. McVicar was the only person with complete knowledge of the recorded conversation.

[59] On at least two previous occasions since October 2013, the current government has faced challenges from the opposition and media with respect to the awarding of personal services contracts[26]. Any suggestion of impropriety in the offering of personal services contracts was historically a significant issue.

---

[26] Shortly after the election in the fall of 2013 questions were raised regarding the decision to hire an unsuccessful liberal candidate as the province's protocol officer using a personal services contract. The opposition raised concerns that such an award was "blatant political payback" (CBC News, Dec. 3, 2013, "Glennie Langille given patronage appointment by Liberals"). In the summer of 2015 there were reports regarding the terms of a Deputy Minister's personal services contract and whether the taxation rate he was subject to as a corporation was appropriate. (Chronicle Herald, September 2, 2015, "Is the idea of public service passé?") In the present case the Auditor General has indicated that he may look into the awarding of personal services contracts. (Global News, November 25, 2015, "N.S. Auditor General considering audit of personal services contracts").

[60] It was in this environment that Mr. McVicar gave media interviews on November 23, 2015.

[61] Mr. McVicar's evidence was that the disclosure of Mr. Younger's personal information on that day was a mistake, a lapse in judgement. In hindsight, he said, it was incorrect. He was trying to describe the state of affairs he was dealing with involving Mr. Younger. He said he was trying to explain why the decisions were made at that time. Mr. McVicar stated that the media were asking him whether he had been trying to bribe Mr. Younger's wife with the offer of a personal services contract. In response to those types of questions, Mr. McVicar explained that he was trying to put into context the Youngers' situation, in an effort to put the allegations to rest.

[62] Mr. Younger's evidence was that he believes the information was disclosed as a "character assassination" intended to undermine his credibility by making him seem unstable. He believes that the Premier's Office was trying to make him seem unstable by suggesting that he had a mental health issue, which he said, undermined his credibility. He believes the intention was to try to end discussion around his situation including discussions regarding the tape recorded conversation with Mr. McVicar. He also stated that he did not think that Mr. McVicar realized he could not (under Nova Scotia's privacy law) disclose his personal information in the way he did.

Cause of the breach – lack of privacy training

[63] In terms of his privacy knowledge, Mr. McVicar stated that he had not received any privacy training during his tenure as Chief of Staff. While he was certain that the Office had a privacy policy and that he had likely received a copy, he had not read it. He did not believe he had signed a confidentiality agreement but thought that there might have been one as part of his employment contract. When asked who was the privacy lead in the Office of the Premier, Mr. McVicar did not know. He also did not know who he would go to if he had a privacy question.

[64] The Communications Director confirmed that he had not received any privacy training and that while he was given a binder of policies - he had not read them. He was uncertain if he had ever signed a confidentiality agreement but thought it might have been part of his personal services contract. When asked who he would go to if he had a privacy question, he said, to his direct report – Mr. McVicar.

[65] The evidence of the remaining witnesses can be summarized as follows:

- When there is a change in government, new staff in the Office of the Premier are provided with transition materials that include a one page information sheet about access to information and privacy contacts and a copy of the Office of the Premier's privacy policy.
- Privacy training at the Office of the Premier and across government is by request. No record is kept of who has received privacy training. The training is not mandatory for any staff. There was a lack of clarity regarding who was responsible for training political

staff. Some witnesses believed the chief of staff could attend deputy minister or cabinet minister trainings and others expressed the belief that political staff would receive their privacy training from the caucus.

- The person primarily responsible for delivering privacy training and answering privacy questions in November 2014 (the Director, Operations and Administration, Premier's Office), reported directly to a number of people including Mr. McVicar.
- As a result of the recent centralization of access and privacy services in government, the point of contact between the Office of the Premier and the new Information Access and Privacy Office within Internal Services is the Executive Director in the Executive Council Office.
- Communications Nova Scotia did not provide any training including any privacy training to the Communications Director in the Office of the Premier.

[66] All civil servants that we spoke to suggested a cultural divide between the actions of political staff and the civil service. There is no evidence to suggest a legal divide – indeed, it is clear that Mr. McVicar was an employee of the Office of the Premier for the purposes of *FOIPOP*, and that the rules in *FOIPOP* governed his collection, use and disclosure of personal information. *FOIPOP* is clear that the Office of the Premier, as a public body, has a duty to ensure reasonable security of the personal information it collects, uses and discloses.[27] This is a duty of the public body and it is given effect by the actions of its individual employees.[28] The consequence of this cultural divide was that there was no clarity and no certainty around who, when, and how privacy training would be provided to political staff in the Office of the Premier.

[67] Had either Mr. McVicar or the Communications Director received privacy training they would most certainly have been immediately aware that the disclosure of personal health information was a significant issue and that, at the very least, they should consult a privacy expert to ensure that any proposed disclosure was authorized under *FOIPOP*. Instead, both individuals were most concerned with ensuring that an explanation was given to any suggestion that there were improprieties with respect to the awarding of personal services contracts. The result was that accountability trumped privacy in a circumstance where the right to privacy no doubt should have prevailed.

Cause of the breach- inadequate media preparation

[68] When asked about his preparation for the interviews he gave on November 23, 2015, Mr. McVicar explained that these were the first media interviews he had given in five years. The Premier had stated in the House that Mr. McVicar would speak if the full recording was released. The full recording was produced on the morning of Nov. 23, 2015, although, as Mr. McVicar points out, the recording does not appear to capture the entire conversation that occurred on the day of the recording. In any event, following the release of the recording, Mr. McVicar stated that there was a pent-up demand from the media to speak to someone about the tape. As a result,

---

[27] *FOIPOP* s. 24(3).

[28] The court stated in *R. v. Morris* (1988), 85 N.S.R. (2d) 200 at 201; "I am of the view that to hold that only a Department can be held in breach of this legislation would make a mockery of the legislation and make if virtually unenforceable…If a member of a Department violated that section, they did so as an agent of the Department".

at 2:00 on the afternoon of November 23, 2015, Mr. McVicar made himself available for media questions.

[69] On November 23, 2015 only the newly appointed Communications Director was available to prepare Mr. McVicar for his media interviews. To prepare for the interviews Mr. McVicar listened a number of times to the audio recording that Mr. Younger had provided to the Speaker's Office that morning. He said he had a brief 10 or 15 minute "back and forth" with the Communications Director but did not prepare any speaking notes. They did not discuss the potential disclosure of Mr. Younger's personal information but did discuss generally that he would talk to the pressures he thought Mr. Younger was under at the time the tape recording was made. Because he had never done these types of interviews before, Mr. McVicar stated that his main preparation was about keeping composure and trying not to ramble. Mr. McVicar's evidence was that he did not think about the privacy implications of what he said. He stated, "I did not think of privacy implications. If I had, I'd still be employed."

[70] The Communications Director for the Office of the Premier in November 2015 had been in that position just one month when he met with Mr. McVicar to help him prepare for his interviews on November 23, 2015. He confirmed that the preparations focussed on the contents of the tape – particularly the personal services contract, and on style and tone. Because the media deadlines were coming up quickly there was little time to prepare. He recalled spending approximately 10 minutes with Mr. McVicar in advance of the interviews. He also stated that no speaking notes were prepared.

[71] The Communications Director recalled that after the first interview in which Mr. McVicar disclosed some personal health information he asked Mr. McVicar if he meant to say that. He did so not because he thought there was a privacy issue but only because they had not talked about disclosing this specific information. Mr. McVicar's response was that it was important for people to understand the context in which decisions were made.

[72] Finally, the Communications Director noted that to a certain extent, the Office of the Premier's staff was taken by surprise by the appearance of the tape. Mr. Younger had sworn an oath before the Clerk of the Legislature saying that no further portion of the tape existed earlier the week before.[29] On that basis they had not anticipated that Mr. McVicar would end up speaking to the press and so no advanced preparation was made for that possibility.

Extent of the breach – sensitivity

[73] Not all personal information is of equal sensitivity. As Nova Scotians we have accepted that personal health information is particularly sensitive personal information.[30] Mental health

---

[29] Mr. Younger referenced this oath in speaking before the Legislature on Friday, November 20, 2015: http://nslegislature.ca/index.php/proceedings/hansard/C96/house_15nov20/; News 957 has reproduced an image of the oath in its news story: http://www.news957.com/2015/11/20/rcmp-investigating-new-secret-recording-made-by-mla-andrew-younger/ .

[30] As I noted earlier, neither *PHIA* nor the rules regarding responding to access to information requests under *FOIPOP* apply here, but both sets of rules are informative. *PHIA* sets very high standards for the collection, use and disclosure of personal health information by health custodians, and *FOIPOP* provides that the disclosure of a

information is considered highly sensitive because there is a stigma associated with mental health diagnoses. The foreseeable harm from the breach included embarrassment, harm to reputation and harm to relationships. As a public figure Mr. Younger also faced a potential loss of trust and respect from constituents and the public generally.

3. Notification

[74] The third step in managing a privacy breach is to determine whether or not notification is necessary. In this case, Mr. Younger was made aware of the disclosure of his personal information before articles began appearing on media websites, broadcasts and blogs. He provided this office with two emails he received from news reporters asking him to confirm the information regarding his medical diagnoses. Notification of the breach in these circumstances would not have provided him with any further useful information about the breach. But effective notification also includes providing other information such as:

- Steps taken so far to control or reduce harm,
- Future steps planned to prevent further privacy breaches,
- Steps individuals can take themselves to reduce harm from the breach,
- Information and Privacy Commissioner contact information,
- Public body contact information – for further assistance.

[75] In this case, a meaningful notification would identify the future steps planned to prevent further privacy breaches. This should include an explanation of how and when the public body intends to implement the recommendations in this report.

Recommendation #1: Breach Notification

[76] That within 30 days of receipt of this report the Office of the Premier:

- provide this office with its response to the recommendations in this report, including timelines for implementation of each recommendation;
- publish its response to the recommendations in this report on its website.

[77] Mr. McVicar both wrote to and visited Mr. Younger shortly after the media interviews to personally apologize to him. While this is not, strictly speaking, a notification, it was an appropriate and respectful gesture. Mr. Younger confirmed that Mr. McVicar had visited him personally shortly after the disclosure of the personal information in order to apologize. Mr. Younger emphasized that he was not out to attack individuals but was concerned generally with preventing similar breaches.

4. Prevention

[78] Once the cause of a breach is investigated and understood, it is important for public bodies to evaluate what steps they can take to prevent future similar breaches. *FOIPOP* requires that

---

person's health care history, diagnosis, condition, treatment or evaluation in response to an access to information request is a presumed unreasonable invasion of personal privacy (*FOIPOP* s. 22).

public bodies protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.[31]

[79] Extensive work has been done across Canada in both the public and private sector on the topic of what steps a public body or organization must take to adequately protect personal information and to prevent or reduce the chance of a privacy breach. There is general agreement that reasonable security provisions in privacy laws require that public bodies develop and implement a privacy management program. This program is intended to ensure that public bodies have built the four pillars of reasonable security: physical controls, technical controls, administrative controls and personnel security controls. [32]

[80] I agree that in order to have reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of personal information, public bodies need to develop and implement a sound privacy management program. Such a program is made up of a combination of public body commitment and program controls.[33]

[81] Witnesses provided evidence relating to the existing privacy management program for government generally and for the Office of the Premier in particular. I reviewed all of the available privacy and access training decks, the privacy policy for the Office of the Premier and the personal services contract and non-disclosure agreement of the chief of staff. The evidence in this case suggests that privacy roles are not clearly communicated, privacy training is not adequate and that privacy policies are dated and not specific enough to be helpful training tools.

[82] In summary the evidence establishes that:

- The Chief of Staff did not attend any privacy training.
- The Director of Communications for the Premier did not attend any privacy training.
- The Chief of Staff was provided with a binder of policies that likely included a privacy policy but he did not read the policy.
- The Director of Communications for the Premier was provided with a binder of policies that likely included a privacy policy but he did not read the policy.
- The Chief of Staff was unaware who the privacy lead within the Office of the Premier was.
- Privacy training is available for government staff but attendance is neither mandatory nor monitored.

---

[31] *FOIPOP* s. 24(3).

[32] For two recent examples, see Office of the Privacy Commissioner of Canada, Special Report to Parliament: Findings under the Privacy Act – Investigation into the loss of a hard drive at Employment and Social Development Canada (March 25, 2014) and Newfoundland and Labrador Report P-2015-002 (November 23, 2015) at paras. 20 & 21. Alberta's Health Information Act (RSA 2000 Chapter H-5) s. 60 also specifically lists administrative, technical and physical safeguards as a requirement for reasonable security.

[33] A summary of the core elements of a sound privacy management program is available on our website in a document entitled, "Privacy Management Program At a Glance" at http://foipop.ns.ca/sites/default/files/PHIA/PMP%20At%20a%20Glance%202015Nov05.pdf.

- Government officials reported that political staff such as the Communications Director and Chief of Staff in the Office of the Premier were expected to get their privacy training from the caucus office.

[83] The Chief of Staff signed a personal services contract and a non-disclosure agreement. Neither document makes specific reference to the application of *FOIPOP*, to privacy laws or to the protection of personal information. This is, in my opinion, a missed important early opportunity to make clear to individuals that their activities under their personal services contract are subject to the privacy rules in *FOIPOP*.

Recommendation #2: Personal Services Contracts

[84] That the standard personal services contract template be updated to add provisions (privacy protection schedule) that:

- clearly state that information obtained by virtue of service to the government is subject to Nova Scotia's access and privacy laws;
- require contractors to complete privacy training within one month of signing of contract and,
- require contractors to sign confidentiality agreements that clearly reference *FOIPOP* access and privacy rules.

Recommendation #3: Non-Disclosure Agreements

[85] That the Employee Non-Disclosure Agreement template be amended to make specific reference to the requirement to protect personal information.

[86] Witnesses gave evidence that political staff, including the Chief of Staff, were provided with privacy information in two primary ways: through transition material and through available privacy training. We obtained a copy of the two documents identified as providing the necessary privacy information during transition and we obtained a copy of all of the access and privacy training presentations given to the Office of the Premier, ministers and deputy ministers in 2013 and 2014.

[87] The transition material on privacy consists of one page entitled, "Freedom of Information" and a copy of the privacy policy. The only reference to privacy in the one page document is a line that says that the person responsible for processing access requests is also available to "manage privacy enquiries and any issues surrounding the protection of privacy, such as privacy breaches". There is no explanation of any privacy rules and readers are not advised that all collection, use and disclosure of personal information by these new staffers are subject to Nova Scotia's privacy laws.

[88] The privacy policy itself was drafted in 2009. It contains two requirements that would have been useful pieces of information for both the Chief of Staff and the Communications Director: that all employees, including those under personal services contracts, are subject to the policy and that all disclosures of personal information will occur only where authorized by law or agreement with other public bodies that are authorized by law. I do not suggest that this is enough information, but it was essential information.

[89] Three different individuals are identified as having some responsibility under the policy:

1. The Corporate IAP/FOIPOP Administrator is required to provide training on proper procedures regarding the privacy of personal information and to monitor compliance with the policy.
2. The Director, Administration, Operations and Special Projects is responsible for making reasonable security arrangements for personal information.
3. The deputy head of the Office of the Premier is accountable for compliance with the policy.

[90] The remainder of the policy is a list of somewhat dated security standards. The policy is in need of updating to more clearly identify exactly when and why personal information is collected, used or disclosed by the Office of the Premier. Readers should understand that any collection, use or disclosure of personal information outside of those circumstances clearly identified in the policy require a consultation with a privacy professional to ensure that the proposed collection, use or disclosure of the personal information is authorized.

[91] The privacy policy includes a breach management protocol. It is unclear whether the protocol was made available to political staff. In addition, the protocol requires updating to ensure that all four key steps for managing privacy breaches are properly addressed. Essential elements such as appropriate risk assessments and proper notification of affected individuals are missing from the protocol. Further, the protocol requires clarity with respect to who is responsible to initiate a privacy investigation when a breach occurs.

Recommendation #4: Privacy Policy

[92] That the Office of the Premier's privacy policy including the breach management protocol be updated to:

- more clearly identify the circumstances in which personal information is collected, used and disclosed by that Office,
- modernize any references to reasonable security standards, and
- update the privacy breach protocol to reflect modern breach management standards.

[93] With respect to the training, some witnesses believed that political staff such as the chief of staff could have attended training given to deputy ministers or ministers. Others said that they would not have attended such training and instead that any privacy training for political staff would have had to come from the caucus. The evidence suggests that there is a cultural divide between political staff and civil servants. This divide created confusion as to who was responsible for ensuring that political staff received essential privacy training.

[94] The evidence established in any event that neither the Chief of Staff nor the Communications Director for the Office of the Premier attended any privacy training.

[95] I reviewed all of the training material supplied by the government. The focus of the training is overwhelmingly on how to manage access to information requests. There is limited

material giving very high level information on privacy. In my opinion, had Mr. McVicar attended any of these trainings it may have increased his awareness of privacy as an issue, but he would not have had sufficient information to know whether or not a disclosure to the media was authorized.

[96] Neither the existing transition material nor the existing training decks provide such essential privacy information as: identifying personal information, understanding the basic rules of when employees are authorized to collect, use or disclose personal information, recognizing a potential privacy issue or breach and knowing exactly to whom employees can address their privacy questions to avoid problems.

Recommendation #5: Privacy Training

[97] That basic privacy training:

- be made mandatory for all government employees and that attendance be monitored;
- be updated to include core elements of: identifying personal information, understanding the basic rules of when employees are authorized to collect, use or disclose personal information, recognizing a potential privacy issue or breach and knowing exactly to whom employees can address their privacy questions to avoid problems. The training should also include essential modern security requirements including end of day procedures, secure destruction of personal information, travelling with personal information and transmitting personal information;
- be periodically refreshed as a mandatory requirement that is monitored and enforced.

[98] That both Mr. McVicar and the Communications Director were unaware of who the privacy lead in the Office of the Premier was suggests a need for clarity around privacy roles. As noted above, there were at least three potential privacy resources available, one of whom reported directly to Mr. McVicar.[34]

[99] A strong, modern privacy management program begins with strong leadership. Appointing a Chief Privacy Officer who occupies an executive-level position provides that leadership. That person's responsibilities would be to oversee and lead the privacy program from a strategic standpoint - to ensure privacy is built into all projects and programs, that resources are dedicated to ensuring that privacy impact assessments are regularly done, that mandatory training is completed, that privacy breaches are managed in accordance with the updated privacy protocol, and that all policies are updated and accurately reflect the current use of personal information. Having a Chief Privacy Officer at a sufficiently influential level in an organization sends the message that privacy is important and is an essential consideration in all decisions involving personal information. Of equal importance is that this high level leadership will ensure that staff, including political staff, will always know where to go with their privacy issues.

---

[34] The Director, Operations and Administration is identified as being responsible for the security of personal information in the privacy policy and gave evidence that she frequently answers privacy related questions from other MLAs and MLA offices. Her evidence was that she reports directly to the Chief of Staff and indirectly to the Deputy Minister.

Recommendation #6: Chief Privacy Officer
[100] That the Office of the Premier and other government public bodies appoint an executive-level Chief Privacy Officer to provide strategic privacy leadership.

[101] I note in closing that the Chief Information Access and Privacy Officer for government gave evidence that significant work is already underway to modernize and improve many aspects of the government's privacy management program including many of the areas identified in this report.

4.0 Summary of Findings and Recommendations

[102] In summary I find:

1. Mr. McVicar, in his role as Chief of Staff to the Premier, was an employee of the Office of the Premier for the purposes of *FOIPOP* and as such, his collection, use and disclosure of personal information was subject to the *FOIPOP* rules.

2. That three pieces of information disclosed by Mr. McVicar to the media on Monday November 23, 2015 were "personal information" within the meaning of *FOIPOP*.

3. That the disclosure of third party personal information by Mr. McVicar on November 23, 2015 was not authorized under *FOIPOP* and as such was a breach of the privacy rules.

Recommendation #1: Breach Notification
[103] That within 30 days of receipt of this report the Office of the Premier:
- provide this office with its response to the recommendations in this report, including timelines for implementation of each recommendation;
- publish its response to the recommendations in this report on its website.

Recommendation #2: Personal Services Contracts
[104] That the standard personal services contract template be updated to add provisions (privacy protection schedule) that:
- clearly state that information obtained by virtue of service to the government is subject to Nova Scotia's access and privacy laws;
- require contractors to complete privacy training within one month of signing of contract and,
- re ,uire contractors to sign confidentiality agreements that clearly reference *FOIPOP* &ccess and privacy rules.

Recommendation #3: Non-Disclosure Agreements
[105] That the Employee Non-Disclosure Agreement template be amended to make specific reference to the requirement to protect personal information.

Recommendation #4: Privacy Policy

[106] That the Office of the Premier's privacy policy including the breach management protocol be updated to:

- more clearly identify the circumstances in which personal information is collected, used and disclosed by that Office,
- modernize any references to reasonable security standards, and
- update the privacy breach protocol to reflect modern breach management standards.

Recommendation #5: Privacy Training

[107] That basic privacy training:

- be made mandatory for all government employees and that attendance be monitored;
- be updated to include core elements of: identifying personal information, understanding the basic rules of when employees are authorized to collect, use or disclose personal information, recognizing a potential privacy issue or breach and knowing exactly to whom employees can address their privacy questions to avoid problems. The training should also include essential modern security requirements including end of day procedures, secure destruction of personal information, travelling with personal information and transmitting personal information;
- be periodically refreshed as a mandatory requirement that is monitored and enforced.

Recommendation #6: Chief Privacy Officer

[108] That the Office of the Premier and other government public bodies appoint an executive-level Chief Privacy Officer to provide strategic privacy leadership.

[109] In one month we will follow up with the Office of the Premier for an update on how it is implementing the recommendations in this report.

5.0 Conclusion

[110] What began as an error in judgement by an individual staffer presents a compelling opportunity for the government. We are experiencing, and will continue to experience, exponential growth in our abilities to collect, use, disclose and store personal information. Being able to do that effectively requires a clear program for managing privacy. Privacy won't happen by accident: it needs strong executive leadership and a clear program for implementation of controls. Implementing the recommendations contained in this report will ensure that the government establishes the foundation for a strong, modern privacy management program.

6.0 Acknowledgements

[111] The Office of the Premier fully cooperated with this investigation. The investigation into this matter was lead by Carmen Stuart, Director of Investigation and Mediation with assistance from Robert Bay, Investigator.

February 11, 2016

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

Appendix 1:
Freedom of Information and Protection of Privacy Act
Summary of Authorities to Disclose Personal Information[35]

Consent provided

Written consent

1. A public body may disclose personal information to anyone if the individual the information is about has identified the information and consented in writing to the disclosure (s. 27(b)).

Consent not required

A public body may disclose personal information without consent in limited circumstances as follows:

Original and compatible purposes

2. For the purpose for which it was obtained or compiled, or a use compatible with that purpose (27(c) and 28 – defines compatible purposes as having a reasonable and direct connection to the original purpose and necessary for operating a legally authorized program).

Disclosures permitted within a public body

3. To an officer or employee of a public body or to a minister if the information is necessary for the performance of the duties of or for the protection of the health or safety of the officer, employee or minister (s. 27(f)).
4. To a public body to meet the necessary requirements of government operation (s. 27(g)).

Next of kin

5. So that next of kin or a friend of an injured, ill or deceased individual may be contacted (s. 27(p)).

Collection of a debt or making payments

6. To collect a debt or fine owing by an individual to the Province or to a public body (s. 27(h)(i)).
7. To make a payment owing by the Province or a public body to an individual (s. 27(h)(ii)).

Health, safety or public interest related disclosures

8. To an officer or employee of a public body or to a minister if the information is necessary for the protection of the health or safety of the officer, employee or minister (s. 27(f)).
9. If the head of the public body determines that compelling circumstances exist that affect anyone's health or safety (s. 27(o)).
10. Where there is a risk of significant harm to the environment or to the health or safety of the public or a group of people or for any other reason, the disclosure is clearly in the public interest (s. 31 – note there are notice requirements set out in s. 31).

[35] Note: It is very important to consult *FOIPOP* directly and to read the specific statutory provision before deciding whether or not it applies in a particular case. This summary is intended only as a simple guide.

Consent not required (cont'd)
A public body may disclose personal information without consent in limited circumstances as follows:
Legal proceedings, law and investigations 11. To respond to an access to information request under *FOIPOP* (s. 27(a)). 12. Pursuant to another enactment (s. 27(a)). 13. To comply with an enactment or with a treaty, arrangement or agreement made pursuant to an enactment (s. 27(d)). 14. To comply with a subpoena, warrant, summons or order (s. 27(e)). 15. To a public body or law enforcement agency in Canada to assist with an investigation undertaken with a view to a law-enforcement proceeding or from which a law-enforcement proceeding is likely to result[36] (s. 27(m)). 16. If the pubic body is a law enforcement agency and the information is disclosed to another law enforcement agency in Canada or in a foreign country under an agreement or legislative authority. (s. 27(n)).
Audits, research, public archives 17. To the Auditor General for audit purposes (s. 27(i)). 18. To a researcher for research or statistical purposes if the requirements of s. 29 are satisfied (s. 27(q)). 19. To the public archives of Nova Scotia or the archives of a public body (s. 27(l)). 20. The public archives of Nova Scotia or of the public body may disclose personal information for archival and historical purposes as set out in s. 30 (s. 27(q)).
MLAs, union representatives 21. To an MLA who has been requested by the individual, whom the information is about, to assist in resolving a problem (s. 27(j)). 22. To a representative of the bargaining agent who has been authorized in writing by the employee whom the information is about, to make an inquiry (s. 27(k)).

[36] "Law enforcement" is defined in s. 3 of *FOIPOP* as policing, including criminal intelligence operations, investigations that lead or could lead, to a penalty or sanction being imposed and proceedings that lead, or could lead, to a penalty or sanction being imposed. "Proceeding" and "investigation" are not defined.